ECS Configuration Change Request

Page 1 of Page(s)

1. Originator Henry Baez	**2. Log Date:** **09/23/03**	**3. CCR #:** **03-0651**	**4. Rev:** **—**	**5. Tel:** 301-925-1025	**6. Rm #:** 2101D	**7. Dept.** Sys Eng

8. CCR Title: Install IBM sendmail binary and associate filesets in VATC firewall first, then on PVC firewall.

9. Originator Signature/Date **Henry Baez /s/ 09/23/03**	**10. Class** **II**	**11. Type:** **CCR**	**12. Need Date:** 9/23/03

13. Office Manager Signature/Date **James R. Mather /s/ 09/23/03**	**14. Category of Change:** Initial ECS Baseline Doc.	**15. Priority:** (If "Emergency" fill in Block 27). Emergency

16. Documentation/Drawings Impacted *(Review and submit checklist):*	**17. Schedule Impact:**	**18. CI(s) Affected:**

19. Release Affected by this Change: 6A	**20. Date due to Customer:**	**21. Estimated Cost:** None - Under 100K

22. Source Reference: □**NCR (attach)** □**Action Item** □**Tech Ref.** □**GSFC** □**Other:**

23. Problem: (use additional Sheets if necessary)
Sendmail contains a buffer overflow in the prescan() function responsible for parsing an email address. By sending a specially crafted email message it is possible to overwrite the stack or heap structures used by the sendmail process. This can allow a remote attacker to execute arbitrary code with the privileges of the sendmail daemon (typically root). Multiple attack vectors can be used to exploit this flaw. Note that since the overflow is triggered by a malicious email message, MTAs not directly facing the Internet are also at risk. This is explained more in CERT Advisory and Vulnerability Note CA-2003-25.

24. Proposed Solution: (use additional sheets if necessary)
IBM has put a temporary fix for our version of OS, AIX 4.3.3. The permanent fix, APAR number for AIX 4.3.3: IY48659, will be issued sometime in October. But the problem is classified as critical so it is highly recommended the program does not wait until October. IBM states that one OS fileset also needs to be upgraded in order to make the sendmail fix work, the bos.net.tcp.client. Install new IBM fileset bos.net.tcp.client.4.3.3.90 and sendmail binary. First install in VATC firewall. Run for a few days to make sure there are no problems then install in PVC firewall. All files will be downloaded directly from IBM, see install instruct

25. Alternate Solution: (use additional sheets if necessary)
None.

26. Consequences if Change(s) are not approved: (use additional sheets if necessary)
We do not actually run IBM sendmail server on firewall, we ran a proxy called smwrap. But we do run the client and as smwrap hands the email over to delivery to sendmail, sendmail has to be fixed to protect internal sendmail servers.

27. Justification for Emergency (If Block 15 is "Emergency"):
According to advisory, if exploited this could case major disruption of email services. If internal servers is compromise, a major incidence to the program could affect a compromise site.

28. Site(s) Affected: □EDF ☒PVC ☒VATC □EDC □ GSFC □LaRC □NSIDC □SMC □AK □JPL
□EOC □ IDG Test Cell □Other

29. Board Comments:	**30. Work Assigned To:**	**31. CCR Closed Date:**

32. EDF/SCDV CCB Chair (Sign/Date): **Byron V. Peters /s/ 09/13/03** **Darryl Washington /s/ 09/13/03**	**Disposition:** [✓ Approved] App/Com. Disapproved Withdraw Fwd/ESDIS ERB Fwd/ECS
33. M&O CCB Chair (Sign/Date):	**Disposition:** Approved App/Com. Disapproved Withdraw Fwd/ESDIS ERB Fwd/ECS
34. ECS CCB Chair (Sign/Date):	**Disposition:** Approved App/Com. Disapproved Withdraw Fwd/ESDIS ERB Fwd/ESDIS

ADDITIONAL SHEET

CCR #: 03-0651 **Rev: — Originator:** Henry Baez

Telephone: 301-925-1025 **Office:** 2101D

Title of Change: Install IBM sendmail binary and associate filesets in VATC firewall first, then on PVC firewall.

See attachment.